5

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/653,191	09/03/2003	Masanori Satake	116971	1739

25944 7590 02/02/2007

OLIFF & BERRIDGE, PLC
P.O. BOX 19928
ALEXANDRIA, VA 22320

EXAMINER
JOHNSON, CARLTON

ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)
	10/653,191	SATAKE ET AL.
	Examiner	Art Unit
	Carlton Johnson	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Response to Remarks

1.1 **Applicant argues** the validity of the 35 U.S.C. 112 second paragraph rejections based on being indefinite and lacking antecedent basis. The terms specified in the previous Office Action were not defined within the Specification or original claims. Each 35 U.S.C. 112 second paragraph rejection is concluded with a statement as to how each term was defined by the Examiner for the prosecution of the application in the Office Action. Since the Applicant has not disputed this interpretation, therefore, the interpretation stands.

1.2 **Applicant argues** that the referenced prior art does not teach or disclose, *" ... a selection unit for selecting one of a first signature key certified by a first certificate authority and a second signature key certified by a second certificate authority ... ". (see Amendment Remarks Page 2, Line 18-20); (see Amendment Remarks Page 3, Lines 1-3)*

By definition, a Certificate Authority (CA) is a security information repository used for the retrieval of a digital certificate, which contains a public encryption key that is used in the generation of a digital signature, signing digital data, and acting as a verifying authority. (see http://whatis.techtarget.com/definition/0,289893,sid9_gci213831,00.html)

The Shear prior art discloses a selection unit based on a software implementation means for the referenced prior art (see Shear col. 3, lines 19-21: software implementation) to select an encryption key for digital signature generation using multiple encryption keys from multiple Certificate Authorities (see Shear col. 4, lines 65-67: multiple CAs). A signature key is equivalent to an encryption key.

As per applicant's own disclosure, the Shear prior art discloses that a verifying authority can sign and certify a load module or instruction data. (see Remarks Page 2, Lines 23-24)

Applicant's disclosure indicates an encryption key for each of the two verifying authorities (i.e. CAs). The Shear prior art discloses multiple (at least two) Certificate Authorities (CA) that can be designated as a first and a second CA. (see Shearer col. 6, lines 62-65: verifying authorities; col. 10, lines 32-34; col. 10, lines 38-40; col. 6, lines 62-65: multiple verifying authorities (i.e. CAs)) In addition, the Shear prior art discloses the capability for each CA to distribute a certificate and a public key within the certificate. (see Shearer col. 10, lines 38-40: multiple verifying authorities (i.e. CA) each with an encryption key; col. 4, 61-67; col. 6, lines 46-52: multiple verification or encryption keys, a first and a second encryption key)

Plus, the Shear prior art discloses a first signature key (i.e. a public or certificate based encryption key utilized for the generation, signing, and verification of a digital signature). (see Shearer col. 10, lines 38-40: multiple verifying authorities (i.e. Certificate Authorities) each with a signature key; col. 4, 61-67; col. 6, lines 46-52: multiple verification or signature keys, a first and a second signature key)

These claim limitations of a selection unit, and multiple CAs plus multiple keys are disclosed by the prior art of record.

1.3 **Applicant argues** that the referenced prior art does not teach or disclose, " *... a judging unit for judging whether or not the next job processor is a device within the network ...* ". *(see Amendment Remarks Page 3, Line 12-13)*

The Shear prior art discloses a judging unit or software means (see Shear col. 3, lines 19-21: software implementation) to implement the prior art. In addition, the Shear prior art discloses the capability to provide an encryption key utilized to generate a digital signature. A domain is defined as a set of network address such as a local area network. The Shear and Teng prior art combination discloses a judging unit (software module) that provides the capability to determine whether a workflow (i.e. job process) is within the present domain or not. A workflow is equivalent to a job process (i.e. instructions to complete a task).

The Shear and Teng prior art combination discloses a workflow (i.e. a job process) that is only accessible by entities within an associated domain or set of interconnected network nodes (see Teng paragraph [0192], lines 1-8: attribute, whether network node within a specific domain, network or outside), and the capability to for a judging unit (i.e. software module) that provides the capability to determine whether a job process is within the present domain or not. In addition, the Shear and Teng prior art combination discloses that a specific signature key is used to in order to access a particular workflow associated with a particular domain, which is equivalent to Applicant's limitation.

This claim limitation of a determination as to whether a job process is within a network or outside is disclosed by the prior art of record.

1.4 **Applicant argues** that the referenced prior art does not teach or disclose, *" ... a signature processor unit for electronically signing the output job flow instruction data using the signature key for the inside when the next job processor is a device within the network and using the signature key for the outside otherwise ... ". (see Amendment Remarks Page 3, Line 13-16)*

The Shear prior art discloses the usage of a first and a second signature key and the usage of multiple CAs. It has been previously established that "within a domain" is equivalent to "within a network" and that the Shear and Teng prior art combination discloses the capability to determine whether a network node is within a domain or outside. The selection of a CA within a domain and the usage of its signature key disclose a signature key within a network.

The claim limitation of a signature key within a network is disclosed by the prior art of record.

1.5 **Applicant argues** that the referenced prior art does not teach or disclose, *" ... a job processor ... ". (see Amendment Remarks Page 3, Line 12-16)*

Applicant's specification discloses the invention is concerned with workflow system. (see Specification paragraphs [0004], [0006]). The Shear and Teng prior art combination discloses a workflow processing environment which is equivalent to the job processing environment utilizing a job processor. (see Shear col. 3, lines 24-32: information processing environment; see Teng paragraph [0192], lines 1-8: workflow environment) The software within the Shear and Teng prior art combination perform equivalent functions to a job processor.

The claim limitation of a job processor is disclosed by the prior art of record.

1.6 **Applicant argues** that the referenced prior art does not teach or disclose, " ... a first signature conversion unit for, when it is determined in the verification by the first verification unit that the electronic signature attached to the document is signed using a signature key for the internal network, deleting the electronic signature from the document, re-attaching an electronic signature to the document using a signature key of the proxy device for the external network ... ". (see Amendment Remarks Page 4, Line 10-14); (see Amendment Remarks Page 4, Lines 20-24); (see Amendment Remarks Page 5, Lines 2-4)

The Shear prior art discloses the capability to use a first or a second signature key to generate and attach (i.e. sign) a digital document. (see Response to Remarks 1.2)

In addition, the Shear prior art discloses the capability to generate and attach a digital signature to a load module containing instructions that are utilized in a job process. (see Shear Figure 5; col. 10, lines 54-59: sign, attach or re-attach a digital signature to a digital document)

The Shear and Shrader prior art combination discloses the capability to delete a digital signature from digital data (i.e. a document). (see Shrader col. 14, lines 24-37:

delete a digital signature) And, the Shear prior art discloses the capability to generate and attach a digital signature to a digital document. (see Shear; col. 10, lines 54-59: sign and attach a digital signature, again) The attached digital can be the first or second attachment of a digital signature to the same digital data (i.e. document).

The claim limitations of the deletion of a digital signature, and attachment are disclosed by the prior art of record.

1.7 The **Shear (6,157,721)**, **Teng (20020138577)**, and **Shrader (6,772,341)** prior art combination discloses all claims limitations, and addresses all of Applicant's arguments dated October 25, 2006, therefore, the rejections based on the referenced prior art are proper and have been upheld.

Claim Issues - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims **2, 4, 7, 10, 12 - 16** are rejected under 35 U.S.C. 112, second paragraph, 37 CFR 1.75(a), as being indefinite for failing to particularly point out and distinctly claim the subject matter, which applicant regards as the invention.

Claim **2** refers to *"unspecified" and "specified" users*, which lacks antecedent basis within the specification. The specification only refers to "unspecified users", and designates "*unspecified users*" as users that are part of the public or are outside the enterprise or company. The Examiner is interpreting *"specified users"* as users that are within the enterprise or company. (see Specification Page 12, Lines 7-11) Appropriate action is required.

Claim **4** refers to *"predetermined",* which lacks antecedent basis within the specification. The term "predetermined" is only used to refer to service processing, error processing, or within name server processing. (see Specification Page 8, Line 8; Page 15, Line 12; Page 16, Line 10; Page 17, Line 11) The term *"predetermined"* is not used within the specification to refer to a network configuration or structure. Claim 4 for this Office Action is interpreted such as a network node contained within a collection of configured nodes constituting a domain. Appropriate action is required.

Claim **7, 10** refer to, *"positional ",* which lacks antecedent basis within the specification. The Specification does not refer to the term "positional". The term "positional" is interpreted to refer to whether the network node is positioned within the protected network environment (i.e. behind a firewall or within an Intranet), or outside the protected network environment (i.e. internetwork, outside of Intranet). Claim 7, 10 for this Office Action is interpreted as the location information of a network node with a network environment. Appropriate correction is required.

Claim **12 - 16** refers to the term *"document"*, which lacks antecedent basis within the specification. The applicant's invention discloses the generation and transfer of instruction data or data to be processed between network nodes for workflow processing. No precise definition of what is contained within a document is given by the specification. Therefore, this particular instruction data or data to be processed is considered analogous to a digital document. Claims **12 - 16** for this Office Action are interpreted as a document disclosure being analogous to the previously disclosed instruction data or data to be processed generated and transferred between network nodes. Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102(b) that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims **1, 2, 5** are rejected under 35 U.S.C. 102(b) as anticipated by **Shear et al.** (US Patent No. **6,157,721**).

With respect to Claims 1, 5, Shear discloses an information processor for instructing a job processor to execute a job process and an information processing method executed by an information processor for instructing a job processor to execute a job process, the information processor and the method comprising the steps of:

a) a selection unit for selecting one of a first signature key certified by a first certificate authority (see Shear col. 10, lines 32-34: Certificate Authority) and a second signature key certified by a second certificate authority (see Shearer col. 10, lines 38-40: multiple verifying authorities (i.e. Certificate Authorities) each with a signature key; col. 4, 61-67; col. 6, lines 46-52: multiple verification or signature keys, a first and a second signature key) for signing instruction data having a process description for instructing a job process or data to be processed (see Shear col. 8, lines 24-28; col. 10, lines 4-8: instructions to be performed, executed) in a job process; *Shear discloses a first and a second certificate authority which are designated as verifying authorities. And, Shear discloses a software module or unit for selection of cryptographic key from Certificate Authority or trusted third party.* (see Shear col. 3, lines 19-21: software implementation; col. 5, lines 43-47: selection of cryptographic key required in order to produce digital signature)

b) a signing unit for signing the instruction data or the data to be processed (see Shear Figure 5; col. 10, lines 4-8: instructions to be performed) using the signature key (see Shear col. 4, lines 61-67; col. 6, lines 46-52: multiple verification or signature keys, a first and a second signature key) selected by the selection unit; *Shear discloses a software module or unit used to sign instruction data.* (see Shear; col. 10, lines 54-59: sign instruction data) and

c) a transmitter unit for transmitting, to the job processor, the instruction data or the data to be processed. *Shear discloses a software module or a unit to transmit signed instruction data.* (see Shear col. 3, lines 19-21: software implementation; col. 10, lines 4-8: instruction data; col. 14, lines 39-41: transfer signed instruction data to processing node)

With respect to Claim 2, Shear discloses an information processor according to claim 1, wherein the certificate authority certifying the first signature key is a certificate authority which certifies unspecified users and the certificate authority certifying the second signature key is a certificate authority which certifies specific users. *Shear discloses a processor using at least two certificate authorities and the capability to distinguish between sets of instruction data based on a digital signature.* (see Shear col. 3, lines 24-32: information processing environment; col. 10, lines 32-34; col. 10, lines 38-40: at least two verifying authorities or Certificate Authorities; col. 6, lines 22-25: different digital signatures for different sets of instruction data, specified users authorized and unspecified users unauthorized)

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims **3, 4, 6 - 11** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Shear et al.** (US Patent No. **6,157,721**) in view of **Teng et al.** (US Patent Application No. **20020138577**).

The Shear and Teng combination discloses a limitation analogous to Applicant's teaching of a digital signature controlling the processing of a workflow attached to a specific network. To begin with, Shear discloses a specific signature key required in order to access a particular workflow or instruction data set. (see Shear Figure 5; col. 3, lines 28-32; col. 8, lines 24-28: load module contains computer program or instruction data set; col. 4, lines 36-37: digital signature controlling execution of load module or instruction data set) And, Teng discloses a workflow that is only accessible by entities within an associated domain defined as an interconnected network of network devices. (see Teng paragraph [0192], lines 1-8: attribute, whether network node within a specific domain, network or an outside, external network) Therefore, the Shear and Teng combination discloses that a specific signature key is required in order to access a particular workflow or instruction data set associated with a particular domain, which is analogous to Applicant's limitation.

With respect to Claim 3, Shear discloses an information processor according to claim 1, wherein the selection unit selects one of the first and second signature keys. Shear does not specifically disclose the selection of a first and second signature key (see Shear col. 4, 61-67; col. 6, lines 46-52: multiple verification or signature keys, a first and a second signature key) based on an attribute of the job processor. Teng discloses a domain, which is defined to be an interconnected network of devices that constitutes an internal network, and the remaining interconnected network of devices that constitutes the outside network. Teng discloses a job processor with an attribute. (see Teng Figure 18, element number 756; paragraph [0192], lines 1-8: attribute, whether network node within a specific domain, network or an outside, external network) *Shear and Teng disclose a first and a second signature key based on an attribute.*

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Teng to attach the usage of instruction data to an Intranet or subset of network nodes. One of ordinary skill in the art would be motivated to employ Teng in order to enable identity based security for a job processing workflow that prevents unauthorized access, reduces congestion by removable of excess traffic within a network environment. (see Teng paragraph [0010], lines 1-15: user identity based security within network environment)

With respect to Claim 4, Shear discloses an information processor according to claim 3, wherein the job processor has an attribute. Shear does not disclose the attribute of a job processor is within a specific network. Shear does not specifically disclose whether the job processor is within a specific network. Teng discloses wherein the attribute of the job processor is whether or not the job processor is located within a predetermined network. (see Teng paragraph [0192], lines 1-8: attribute, whether network node within a specific domain, network or an outside, external network; paragraph [0193], lines 1-5; paragraph [0193], lines 11-16: job processor attribute) A domain as specified in Teng as defined to be a group of networked computers or a network that share a common communications address.

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Teng to attach the usage of instruction data to an Intranet or subset of network nodes. One of ordinary skill in the art would be motivated to employ Teng in order to enable identity based security for a job processing workflow that prevents unauthorized access, reduces congestion by removable of excess traffic within a network environment. (see Teng paragraph [0010], lines 1-15: user identity based security within network environment)

With respect to Claim 6, Shear discloses a job processor for executing a service in cooperation with other job processors according to job flow instruction data, the job processor comprising:

c) a signature verification unit for verifying an electronic signature attached to the job flow instruction data received at the receiver unit; (see Shear Figure 6; col. 9, lines 58-64: verify signature, process module if digital signature authorized)

d) a processor unit for identifying, from the job flow instruction data, a process instruction the job processor should execute when the verification by the signature verification unit is successful and for executing the process according to the process instruction; (see Shear col. 8, lines 24-28: executable instruction data)

g) a signature processor unit for electronically signing the output job flow instruction data using the signature key for the inside when the next job processor is a device within the network and using the signature key for the outside otherwise; (see Shear Figure 5; col. 10, lines 54-59: sign instruction data) and

h) a transmitter unit for transmitting the output job flow instruction data electronically signed by the signature processor unit to the next job processor. (see Shear col. 3, lines 24-27: local or remote transmission; col. 14, lines 39-41: transfer signed instruction data to processing node)

Shear discloses a job processor utilizing digital signature keys. (see Shear col. 10, lines 38-40; col. 6, lines 22-25; col. 6, lines 49: multiple CAs, multiple signature keys) Shear does not specifically disclose the concept of a network configuration designating data transferred inside a specific network, domain or outside a specific network.

However, Teng discloses:

a) a key storage unit having separate signature keys, one for use inside of a network to which the job processor belongs and the other for use outside of the network; (see Teng paragraph [0192], lines 1-8: network node within a specific network, domain or an outside, external network; paragraph [0403], lines 1-5: key information storage)

b) a receiver unit for receiving job flow instruction data which indicates a process instruction for each job processor and a next job processor for each job process; (see Teng paragraph [0202], lines 17-20: next job process or application designated in workflow processing)

e) an instruction data creation unit for creating output job flow instruction data to be transmitted to a next job processor based on the received job flow instruction data when the process is executed by the processor unit; (see Teng paragraph [0189], lines 1-10: instruction data generation)

f) a judging unit for judging whether or not the next job processor is a device within the network; (see Teng paragraph [0192], lines 1-8: determination job processor within a specific network, domain or an outside, external network)

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Teng to attach the usage of instruction data to an Intranet or subset of network nodes. One of ordinary skill in the art would be motivated to employ Teng in order to enable identity based security for a job processing workflow that prevents unauthorized access, reduces congestion by removable of excess traffic within a network environment. (see Teng paragraph [0010], lines 1-15: user identity based security within network environment)

With respect to Claim 7, Teng discloses a job processor according to claim 6, wherein the judging unit judges whether or not the next job processor is a device within the network based on positional information of the next job processor on the internet indicated in the job flow instruction data. (see Teng paragraph [0202], lines 17-20: determination next job processor or application; paragraph [0192], lines 1-8: determine job processor within a specific network, domain or an outside, external network)

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Teng to attach the usage of instruction data to an Intranet or subset of network nodes. One of ordinary skill in the art would be motivated to employ Teng in order to enable identity based security for a job processing workflow that prevents unauthorized access, reduces congestion by removable of excess traffic within a network environment. (see Teng paragraph [0010], lines 1-15: user identity based security within network environment)

With respect to Claim 8, Shear discloses a method for processing job flow instruction data in a job processor for executing a service in cooperation with other job processors according to the job flow instruction data, the method comprising the steps of:

b) verifying an electronic signature attached to the received job flow instruction data; (see Shear Figure 6; col. 9, lines 58-61: verify signature)

c) identifying a process instruction which should be executed by the job processor from the job flow instruction data when verification is successful; (see Shear col. 9, lines 61-64: verify signature and process module if digital signature is authorized)

d) executing a process according to the identified process instruction; (see Shear col. 9, lines 61-64: execute instruction data)

h) transmitting the electronically signed output job flow instruction data to the next job processor. (see Shear col. 3, lines 24-27: local or remote transmission; col. 14, lines 39-41: transfer signed instruction data to processing node)

Shear discloses a job processor with a digital signature capability and electronically signing the output job flow instruction data using a signature key (see Shear Figure 5; col. 10, lines 54-59: sign instruction data). Shear does not specifically disclose the determination of whether a processor is within a specific network or the next job processor in workflow.

However, Teng discloses:

a) receiving job flow instruction data which indicates a process instruction for each job processor and a next job processor for each job process; (see Teng paragraph [0192], lines 1-2: next instruction data or application indicated in workflow for processing)

e) creating, when the process instruction is executed, output job flow instruction data to be transmitted to the next job processor based on the received job flow instruction data; (see Teng paragraph [0195], lines 10-12: next job flow based on previous job flow)

f) judging whether or not the next job processor is a device within the network; (see Teng paragraph [0192], lines 1-8: determination job processor within a specific network, domain or an outside, external network)

g) using a signature key for the inside of the network to which the job processor belongs when the next job processor is a device within the network and a signature key for outside the network otherwise; (see Teng paragraph [0192], lines 1-8: determination job processor within a specific network, domain or an outside, external network)

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Teng to attach the usage of instruction data to an Intranet or subset of network nodes. One of ordinary skill in the art would be motivated to employ Teng in order to enable identity based security for a job processing workflow that prevents unauthorized access, reduces congestion by removable of excess traffic within a network environment. (see Teng paragraph [0010], lines 1-15: user identity based security within network environment)

With respect to Claim 9, Shear discloses an instruction data creating device for creating job flow instruction data which indicates a process instruction for each job processor and a next job processor for each job process for a system for realizing a service by sequentially sending the job flow instruction data among the job processors and each job processor sequentially executing the process instruction for the job processor, the device comprising:

d) a transmitter unit for transmitting the job flow instruction data electronically signed by the signature processor unit to a first job processor among the job processors for the service. (see Shear col. 3, lines 24-27: local or remote transmission; col. 14, lines 39-41: transfer signed instruction data to processing node)

Shear discloses a signature processor unit for electronically signing the job flow instruction data. (see Shear Figure 5; col. 10, lines 54-59: sign instruction data) Shear does not specifically disclose the capability to determine instruction data processing within a specific network, domain or an outside, external network. However, Teng discloses:

a) a key storage unit having a signature key for inside the network to which the instruction data creating device belongs and a signature key for outside the network; (see Teng paragraph [0403], lines 1-5: key information storage)

b) a judgment unit for judging whether or not a job processor outside the network exists among the job processors for the service; (see Teng paragraph [0192], lines 1-8: determination job processor within a specific network, domain or an outside, external network)

c) using the signature for outside the network when the judgment unit judges that there is a device which is outside the network in the job processors for the service and using the signature for the inside otherwise; (see Teng paragraph [0192], lines 1-8: determination job processor within a specific network, domain or an outside, external network)

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Teng to attach the usage of instruction data to an Intranet or subset of network nodes. One of ordinary skill in the art would be motivated to employ Teng in order to enable identity based security for a job processing workflow that prevents unauthorized access, reduces congestion by removable of excess traffic within a network environment. (see Teng paragraph [0010], lines 1-15: user identity based security within network environment)

With respect to Claim 10, Teng discloses an instruction data creating device according to claim 9, wherein the judgment unit judges whether or not the next job processor is within the network based on positional information of the next job processor on the Internet indicated in the job flow instruction data. (see Teng paragraph [0192], lines 1-8: determination job processor within a specific network, domain or an outside, external network)

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Teng to attach the usage of instruction data to an Intranet or subset of network nodes. One of ordinary skill in the art would be motivated to employ Teng in order to enable identity based security for a job processing workflow that prevents unauthorized access, reduces congestion by removable of excess traffic within a network environment. (see Teng paragraph [0010], lines 1-15: user identity based security within network environment)

With respect to Claim 11, Shear disclose a method in which a computer system creates job flow instruction data which indicates a process instruction for each job processor and a next job processor for each job processor for a system for realizing a service by sequentially sending the job flow instruction data among the job processors and each of the job processors sequentially executing the process instruction for the job processor, the method comprising the steps of:

c) transmitting the electronically signed job flow instruction data to a first job processor of the job processors for the service. (see Shear col. 3, lines 24-27: remote or local; col. 14, lines 39-41: transfer signed instruction data to processing node)

Shear discloses electronically signing (see Shear Figure 5; col. 10, lines 54-59: sign instruction data) the job flow instruction data using a signature key. Shear does not specifically disclose the capability to determine whether inside a specific network or an outside, external network.

However, Teng discloses:

a) judging whether or not a job processor outside a network to which the computer system belongs exists among the job processors for the service; (see Teng paragraph [0192], lines 1-8: determination job processor within a specific network, domain or an outside, external network)

b) using a signature key for the outside of the network when it is judged that there is a device which is outside the network in the job processors for the service and a signature key for the inside the network otherwise; (see Teng paragraph [0192], lines 1-8: attribute, whether network device within a specific network, domain or an outside, external network)

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Teng to attach the usage of instruction data to an Intranet or subset of network nodes. One of ordinary skill in the art would be motivated to employ Teng in order to enable identity based security for a job processing workflow that prevents unauthorized access, reduces congestion by removable of excess traffic within a network environment. (see Teng paragraph [0010], lines 1-15: user identity based security within network environment)

8. Claims **12 - 16** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Shear et al.** (US Patent No. **6,157,721**) in view of **Teng et al.** (US Patent Application No. **20020138577**) and further in view of **Shrader et al.** (US Patent No. **6,772,341**).

With respect to Claim 12, Shear discloses a first signature conversion unit for, when it is determined in the verification by the first verification unit that the electronic signature attached to the document is signed using a signature key (see Shear Figure 6; col. 9, lines 58-64: verify signature, process module if digital signature is authorized) for the internal network, re-attaching an electronic signature to the document using a signature key (see Shear Figure 5; col. 10, lines 54-59: sign document)

In addition, Shear discloses:

a) a first signature verification unit for verifying an electronic signature attached to a document transmitted from the device on the internal network to the device on the external network; (see Shear Figure 6; col. 9, lines 58-64: verify signature, process module if digital signature is authorized)

c) a transmitter unit for transmitting the electronically signed document to the device on the external network. (see Shear col. 3, lines 24-27: remote or local; col. 14, lines 39-41: transfer signed document to processing node)

Instruction data is a digital representation of information. A document stored in electronic form is also a digital representation of information. Therefore, instruction data disclosed in Shear is analogous to a document disclosed in applicant's invention. Shear does not specifically disclose the capability to delete an attached digital signature from a document or the capability to determine whether a document is within specific network, domain or a proxy device.

However, Teng discloses a domain which is defined to be an interconnected network of devices which constitutes an internal network and the remaining interconnected network of network devices constitutes the outside network or an external network.

In addition, Teng discloses a proxy device (see Teng paragraph [0133], lines 4-7: proxy interface) provided between an internal network and an external network, for exchanging documents between a device on the internal network and a device on the external network, comprising:

b) the proxy device for the external network (see Teng paragraph [0133], lines 4-7: proxy interface; paragraph [0192], lines 1-8: attribute, whether network node within a specific network, domain or an outside, external network;

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Teng to attach the usage of an instruction data set to an Intranet or a subset of network nodes. One of ordinary skill in the art would be motivated to employ Teng in order to enable identity based security for a job processing workflow that prevents unauthorized access, reduces congestion by removable of excess traffic within a network environment (see Teng paragraph [0010], lines 1-15: user identity based security within network environment).

The combination of Shear and Teng does not specifically disclose the capability to delete an attached digital signature from a document.

However, Shrader discloses deleting the electronic signature from the document (see Shrader col. 14, lines 24-37: delete signature information).

The usage of standards enables interoperability within a heterogeneous distributed network environment. Usage of the PKCS number 7 standard (PKCS # 7) enables implementation of a cryptographic system within a certificate based key management environment and enables the usage of arbitrary attributes such as a signing time for additional authentication capabilities in order to effectively determinate certificate expiration data for strengthened security.

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Shrader to delete an attached digital signature from a document. One of ordinary skill in the art would be motivated to employ Shrader in order to utilized standards based processing techniques to improved data processing (see Shrader col. 3, lines 31-35; col. 2, lines 25-29; col. 2, lines 31-32: standards based data processing, PKCS # 7 standard)).

With respect to Claim 13, Shear discloses according to claim 12, further comprising:

a second signature verification unit for verifying an electronic signature (see Shear Figure 6; col. 9, lines 58-64: verify signature, process module if digital signature is authorized) attached to a document transmitted. In addition, Shear discloses when verification by the second signature verification unit is successful (see Shear Figure 6; col. 9, lines 58-64: verify signature, process module if digital signature is authorized), the electronic signature from the document, re-attaching an electronic signature to the document using a signature key of the proxy device for the internal network; (see Shear Figure 5; col. 10, lines 54-59: sign document), and a transmitter unit for transmitting the electronically signed document to the device on the internal network. (see Shear col. 14, lines 39-41: transfer signed instruction data to processing node) Shear does not specifically disclose a proxy device, the capability to determine whether a document is attached to an internal or an external network, and the capability to delete an attached digital signature from a document.

However, Teng discloses:

a) a proxy device (see Teng paragraph [0133], lines 4-9: proxy interface), a document transmitted (see Teng paragraph [0101], lines 5-7: ftp protocol used for a document transmission) from a device on the external network to a device on the internal network; (see Teng paragraph [0192], lines 1-8: attribute, whether network node within specific network, domain or outside specific network)

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Teng to attach the usage of an instruction data set to an Intranet or a subset of network nodes. One of ordinary skill in the art would be motivated to employ Teng in order to enable identity based security for a job processing workflow that prevents unauthorized access, reduces congestion by removable of excess traffic within a network environment (see Teng paragraph [0010], lines 1-15: user identity based security within network environment).

The combination of Shear and Teng does not specifically disclose the capability to delete an attached digital signature from a document.

However, Shrader discloses:

b) a second signature conversion unit for deleting (see Shrader col. 14, lines 24-37: delete signature information)

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Shrader to delete an attached digital signature from a document. One of ordinary skill in the art would be motivated to employ Shrader in order to utilized standards based processing techniques to improved data processing (see Shrader col. 1, lines 22-25; col. 3, lines 31-35: standards based data processing).

With respect to Claim 14, Shear discloses verifying an electronic signature (see Shear Figure 6; col. 9, lines 58-64: verify signature, process module if digital signature is authorized) attached to a document. Shear does not specifically disclose a proxy device, the concept of an internal and an external network, or the deletion of an attached digital signature from a document comprising the steps of:

c) re-attaching an electronic signature to the document from which the electronic signature has been deleted using a signature key of the proxy device for the external network; (see Shear Figure 5; col. 10, lines 54-59: sign, attach or re-attach instruction data) and

d) transmitting the document to which an electronic signature is re-attached using the signature key for the external network to the device on the external network. (see Shear col. 14, lines 39-41: transfer signed instruction data to processing node)

The deletion of an attached digital signature from an available signed document is a convenience which enables the usage of the current document for the attachment of a different digital signature. It would have been obvious to one skilled in the art to enable the capability to delete an attached digital signature as a worthwhile capability and a great convenience as taught by Shrader. This particular capability negates the need to acquire the original document in order to attach a different digital signature, since acquisition of the original document may not be possible.

Shear does not specifically disclose a method for exchanging or transmitting, in a proxy device provided between an internal network and an external network, documents between a device on the internal network and a device on the external network.

However, Teng discloses:

a) a document transmitted from a device on the internal network to a device on the external network; (see Teng paragraph [0101], lines 5-7: ftp protocol used to transmit a document; paragraph [0192], lines 1-8: attribute, whether network node within a specific network, domain or an outside, external network)

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Teng to attach the usage of an instruction data set to an Intranet or a subset of network nodes. One of ordinary skill in the art would be motivated to employ Teng in order to enable identity based security for a job processing workflow that prevents unauthorized access, reduces congestion by removable of excess traffic within a network environment (see Teng paragraph [0010], lines 1-15: user identity based security within network environment).

The combination of Shear and Teng does not specifically disclose the capability to delete a signature from a document.

However, Shrader discloses:

b) deleting the electronic signature from the document when it is determined in the verification that the electronic signature attached to the document is signed using a signature key for the internal network; (see Shrader col. 14, lines 24-37: delete signature information)

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Shrader to delete an attached digital signature from a document. One of ordinary skill in the art would be motivated to employ Shrader in order to utilized standards based processing techniques to improved data processing (see Shrader col. 1, lines 22-25; col. 3, lines 31-35: standards based data processing).

With respect to Claim 15, Shear discloses a signature verification unit (see Shear Figure 6; col. 9, lines 58-64: verify signature, process module if digital signature is authorized) for verifying an electronic signature. Shear discloses re-attaching an electronic signature to the document using a signature key for the internal network; (see Shear Figure 5; col. 10, lines 54-59: sign, attach, re-attach digital signature to instruction data or document).

Shear does not specifically disclose a proxy device or the concept of an internal and an external network or the deletion of an attached digital signature from a document.

However, Teng discloses a proxy device (see Teng paragraph [0133], lines 4-9: proxy interface) provided between an internal network and an external network for exchanging documents between a device on the internal network and a device on the external network, the proxy device comprising:

a) a document transmitted from a device on the external network to a device on the internal network; (see Teng paragraph [0101], lines 5-7: ftp protocol used to transmit a document between network devices; paragraph [0192], lines 1-8: determination job processor within a specific network or an outside, external network)

c) a transmitter unit for transmitting the document to the device on the internal network. (see Teng paragraph [0101], lines 5-7: ftp protocol used to transmit a document between network devices)

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Teng to attach the usage of an instruction data set to an Intranet or a subset of network nodes. One of ordinary skill in the art would be motivated to employ Teng in order to enable identity based security for a job processing workflow that prevents unauthorized access, reduces congestion by removable of excess traffic within a network environment (see Teng paragraph [0010], lines 1-15: user identity based security within network environment).

The combination of Shear and Teng does not specifically disclose the deletion of a digital signature from a document.

However, Shrader discloses:

b) a signature conversion unit for deleting, when verification by the signature verification unit is successful, the electronic signature from the document (see Shrader col. 14, lines 24-37: delete signature information),

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Shrader to delete an attached digital signature from a document. One of ordinary skill in the art would be motivated to employ Shrader in order to utilized standards based processing techniques to improved data processing (see Shrader col. 1, lines 22-25; col. 3, lines 31-35: standards based data processing).

With respect to Claim 16, Shear discloses verifying an electronic signature (see Shear Figure 6; col. 9, lines 58-64: verify signature, process module if digital signature is authorized) attached to a document.

Shear discloses a method for changing, in a proxy device provided between an internal network and an external network, documents between a device on the internal network and a device on the external network, the method comprising the steps of:

c) re-attaching an electronic signature to the document from which the electronic signature is deleted using a signature key of the proxy device for the internal network; (see Shear Figure 5; col. 10, lines 54-59: sign, attach or re-attach signature to document)

Shear does not specifically disclose a proxy device, the capability to attach a document to a specific network or domain, or the deletion of a digital signature from a document.

However, Teng discloses:

a) transmitted from a device on the external network to a device on the internal network; (see Teng paragraph [0101], lines 5-7: ftp protocol used to transmit a document between network devices; paragraph [0192], lines 1-8: determination job processor within a specific network, domain or an outside, external network)

d) transmitting the document having an electronic signature re-attached using the signature key for the internal network to the device on the internal network. (see Teng paragraph [0101], lines 5-7: ftp protocol used to transmit a document)

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Teng to attach the usage of an instruction data set to an Intranet or a subset of network nodes. One of ordinary skill in the art would be motivated to employ Teng in order to enable identity based security for a job processing workflow that prevents unauthorized access, reduces congestion by removable of excess traffic within a network environment (see Teng paragraph [0010], lines 1-15: user identity based security within network environment).

The combination of Shear and Teng does not specifically disclose the deletion of a digital signature from a document.

However, Shrader discloses:

b) deleting the electronic signature from the document when the verification is successful; (see Shrader col. 14, lines 24-37: delete signature)

It would have been obvious to one of ordinary skill in the art to have modified Shear as taught by Shrader to delete an attached digital signature from a document. One of ordinary skill in the art would be motivated to employ Shrader in order to utilized standards based processing techniques to improved data processing (see Shrader col. 1, lines 22-25; col. 3, lines 31-35: standards based data processing).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton Johnson whose telephone number is 571-270-1032. The examiner can normally be reached Monday through Friday from 8:00AM to 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar Moazzami, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

C.J.
Carlton Johnson
January 18, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/21/07